This document is scheduled to be published in the Federal Register on 03/29/2022 and available online at **federalregister.gov/d/2022-06548**, and on **govinfo.gov**

BILLING C

NATIONAL ARCHIVES AND RECORDS ADMINISTRATION

Information Security Oversight Office

32 CFR Part 2001

[FDMS No. NARA-22-0002; NARA-2022-021]

RIN 3095-AC06

Classified National Security Information

AGENCY: Information Security Oversight Office (ISOO), National Archives and Records Administration (NARA).

ACTION: Direct final rule.

SUMMARY: We are revising our Classified National Security Information regulation to permit digital signatures that meet certain requirements on the Standard Form (SF) 312, which is the non-disclosure agreement required prior to accessing classified information. Due to agency needs during the COVID-19 pandemic and remote work situations, combined with developments in digital signatures since a regulatory prohibition on electronic signatures was implemented in 2010, it is both urgent and appropriate to make this administrative change at this time.

DATES: This rule is effective on [INSERT DATE 40 DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER], unless we receive adverse comments by [INSERT DATE 30 DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER] that warrant revising or rescinding this rulemaking.

ADDRESSES: You may submit comments, identified by RIN 3095-AC06, by the following method:

• *Federal eRulemaking Portal*: https://www.regulations.gov. Search for RIN 3095-AC06 and follow the site's instructions for submitting comments.

We may publish any comments we receive without changes, including any personal information you include.

During the COVID-19 pandemic and remote work situation we cannot accept comments my mail or delivery because we do not have staff in the office.

FOR FURTHER INFORMATION CONTACT: Kimberly Keravuori, Regulatory and External Policy Program Manager, by email at regulation_comments@nara.gov, or by telephone at 301.837.3151.

SUPPLEMENTARY INFORMATION: These regulations were last revised in 2010. At that time, these regulations included a prohibition against signing the Standard Form (SF) 312 electronically, due to concerns about integrity and legal enforceability of any form of electronic signature (e-signature) at the time. In the decade-plus since then, encryption and other measures for e-signatures have advanced and they are now regularly encouraged or required and deemed legally enforceable. In addition, Federal agencies are required to digitize services and forms and accelerate the use of e-signatures as much as possible (*see, e.g.,* 2018 21st Century Integrated Digital Experience Act (21st Century IDEA), 44 U.S.C. 3501 note).

Since the COVID-19 pandemic began in March 2020, numerous Federal agencies have had to engage in remote work to varying degrees and have had difficulty bringing new workers onboard who require access to classified information, due to the requirement for handwritten signatures on the SF 312. It has been placing employees at risk of spreading the virus, as well as creating logistical and other difficulties. Multiple agencies have been consistently requesting the ability to allow e-signatures as a result, and the need became critical and urgent once the COVID-19 pandemic extended much longer than originally anticipated.

The advances in technical ability to ensure valid e-signatures, and legal acceptance of such signatures, is clearly the way of the future and necessary to support a modernized classified national security information system. However, the timing to make this change is more urgent now because of COVID-19 related health risks.

Under laws such as the Government Paperwork Elimination Act (GPEA), 44 U.S.C. 3504 note, the Uniform Electronic Transactions Act (UETA), a model act since adopted by 47 states and the

District of Columbia (the remaining three states have comparable laws), and the Electronic Signatures in Global and National Commerce Act (ESIGN), 15 U.S.C. 7001, *et seq*., an e-signature has the same legal weight as a handwritten signature and cannot be considered invalid simply due to being electronic. The laws establish criteria for valid e-signatures, along the following lines: intent to sign, consent to do business electronically, association of the signature with the record, attribution to the person signing, and a record of the digital transactions. The United States practices an open-technology approach, meaning there's no law requiring use of a specific signing technology for an e-signature to be legally binding, as long as it meets the criteria.

However, for the purpose of e-signatures on the SF 312, ISOO has established certain requirements agencies must meet if they wish to allow such signatures. We require that agencies use digital signatures (rather than other forms of e-signature) on the SF 312 because digital signatures provide the requisite level of security and authenticity appropriate for these agreements. Digital signatures are a specific signature technology type of e-signature that allows users to sign documents and authenticate the signer. Digital signatures are based on a standard, accepted format, called public key infrastructure (PKI), to provide the highest levels of security and universal acceptance through use of a mathematical algorithm and other features. The mathematical algorithm acts like a cipher and encrypts the data matching the signed document. The resulting encrypted data is the digital signature, which is also marked with the time the document was signed and is invalidated if the document is changed after signing. To protect the integrity of the signature, PKI also includes other requirements, including a reliable certificate authority (CA) that can ensure key security and provide necessary digital certificates.

The PKI and CA combination used for digital signatures ensures authentication (*i.e.,* that the digital signature was made by the person it claims to have been made by); consent (*i.e.,* that the person who digitally signed the form meant to do so); and integrity (*i.e.,* that the SF 312 has not changed since the signature was made). As a result, we require agencies to use digital signatures

if they allow e-signatures on their SF 312s. Digital signatures created using Federal Government personal identity verification (PIV) cards or common access cards (CACs) require the card holder to enter their personal identification number (PIN), and meet the requirements outlined above, so it is possible for Federal employees and contractors with such cards to digitally sign the SF 312 using these cards. Agencies may choose to use other digital signature providers than the PIV or CAC cards, as long as they meet the same requirements.

The existing SF 312 has been approved by the General Services Administration (GSA) as a standard form. In conjunction with this rulemaking action, we are working with the appropriate agencies to revise the form to make it electronically fillable and to allow digital signatures.

Regulatory analysis

Administrative procedure

Under the Administrative Procedure Act, an agency may waive the normal notice and comment procedures if the action is a rule of agency organization, procedure, or practice. See 5 U.S.C. 553(b)(3)(A). Since this rule modifies administrative procedures and practice regarding how agencies may allow a form to be signed and maintained, notice and comment are not necessary.

Executive Order 12866, Regulatory Planning and Review, and Executive Order 13563, Improving Regulation and Regulation Review

The Office of Management and Budget (OMB) has reviewed this rulemaking and determined it is not "significant" under section 3(f) of Executive Order 12866. It is not significant because it is a rule of agency procedure and practice, describing our procedures for agencies to handle and process the Standard Form (SF) 312, and we do not anticipate it having an economic impact on the public. It will help ensure easier onboarding and access to classified information for employees and contractors, safeguard employees and others from risks of COVID infection, reduce logistical complications and difficulties during the pandemic and thereafter, and update the form's procedures for easier use with current technological developments.

Regulatory Flexibility Act (5 U.S.C. 601, et seq.)

This review requires an agency to prepare an initial regulatory flexibility analysis and publish it when the agency publishes the rule. This requirement does not apply if the agency certifies that the rulemaking will not, if promulgated, have a significant economic impact on a substantial number of small entities (5 U.S.C. 603). We certify, after review and analysis, that this rulemaking will not have a significant adverse economic impact on small entities.

Paperwork Reduction Act of 1995 (44 U.S.C. 3501, et seq.)

The Paperwork Reduction Act of 1995 (PRA) (44 U.S.C. 3501, *et seq*.) requires that agencies consider the impact of paperwork and other information collection burdens imposed on the public and, under the provisions of PRA section 3507(d), obtain approval from OMB for each collection of information we conduct, sponsor, or require through regulations. The existing SF 312 is such an information collection and has already been approved by OMB/GSA. This rulemaking does not impose additional information collection requirements on the public.

Executive Order 13132, Federalism

Executive Order 13132 requires agencies to ensure state and local officials have the opportunity for meaningful and timely input when developing regulatory policies that may have a substantial, direct effect on the states, on the relationship between the Federal Government and the states, or on the distribution of power and responsibilities among the various levels of government. If the effects of the rule on state and local governments are sufficiently substantial, the agency must prepare a Federal assessment to assist senior policy makers. This rulemaking will not have any effects on state and local governments within the meaning of the E.O. Therefore, no federalism assessment is required.

Unfunded Mandates Reform Act (Sec. 202, Pub. L. 104-4; 2 U.S.C. 1532)

The Unfunded Mandates Reform Act requires that agencies determine whether any Federal mandate in the rulemaking may result in state, local, and tribal governments, in the aggregate, or

the private sector, expending $100 million in any one year. This rule does not contain a Federal mandate that may result in such an expenditure.

List of Subjects in 32 CFR Part 2001

Archives and records, Records disposition, Records management, Records schedules, Reporting and recordkeeping requirements, Scheduling records.

For the reasons stated, NARA amends 32 CFR part 2001 as follows:

PART 2001 – CLASSIFIED NATIONAL SECURITY INFORMATION

1. The authority citation for part 2001 continues to read as follows:

Authority: Sections 5.1(a) and (b), E.O. 13526, (75 FR 707, January 5, 2010).

2. Amend § 2001.80 by:

a. Revising paragraph (d)(2)(ii);

b. In paragraph (d)(2)(v), adding a sentence to the end of the paragraph; and

c. In paragraph (d)(2)(vii), adding the parenthetical "(either in paper form or electronic form)" to the second sentence, in between the words "The original" and ", or a legally enforceable facsimile".

The revision and addition read as follows:

§ 2001.80 Prescribed standard forms.

*****

(d) ***

(2) ***

(ii) The SF 312 may be filled out electronically or by hand, then must be signed. It may be signed by hand and scanned, if the implementing agency permits and the scanned version is done in a way that constitutes a legally enforceable facsimile. Alternatively, the form may be digitally signed if the implementing agency permits, and if the digital signature mechanism employs public key cryptography in a way that meaningfully guarantees authenticity (*i.e.,* that the digital signature was made by the person it claims to have been made by); consent (*i.e.,* that the person

who digitally signed the form meant to do so); and integrity (*i.e.,* that the SF 312 has not changed since the signature was made). Digital signatures created using Personal Identity Verification (PIV) cards or common access cards (CACs) issued by the U.S. Government that are compliant with Homeland Security Presidential Directive 12 (HSPD-12), or its successor, meet the requirements of this paragraph (d)(2)(ii). They include public key infrastructure (PKI), digital signature certificates issued by a certificate authority (CA), and a PIN the signer must enter in order to digitally sign. Agencies may choose to use other digital signature mechanisms than the PIV or CAC cards, as long as they meet the requirements of this paragraph (d)(2)(ii). The form may not be signed using other forms of electronic signature (e-signature), such as typing "/s/ [first and last name]" or attaching an image of a handwritten signature.

*****

(v) *** If the SF 312 is digitally signed, it does not require a witness to observe and verify the digital signature, and therefore also does not require an official to subsequently accept the signature.

*****

David S. Ferriero,

Archivist of the United States.

[FR Doc. 2022-06548 Filed: 3/28/2022 8:45 am; Publication Date: 3/29/2022]